DoD Certification and Accreditation

- Overview
- Defense in Depth
- Terms
- Accreditation Process
- Orange Book – DOD 5200.28 – Trusted Computer Security Evaluation Criteria
- Common Criteria
- DOD Information Technology Security Certification and Accreditation Process (DITSCAP)
- SIPRNET Connection Approval Process
- Red/Black Installation Guide

DOD Information Assurance

DOD Security Policy -- “Defense in Depth”

- Physical Security
- Procedural Security
- Computer Security
- Operational Security
- Personnel Security
- Communication Security
- Information Security

DoD Defense in Depth NIPRNET Style

- Classified “Defense in Depth” refers to the previous slide where it is more than automation
- NIPRNET Defense in Depth normally refers to only automation
  - Firewalls
  - Intrusion Detection Systems
  - PKI/Public Key
  - DMZs

Defense in Depth

ISEC's Approach to

"Defense in Depth"

Level 1 Security - Perimeter (WAN Interface)

High Level Packet Filtering of Commonly Understood Vulnerabilities

- -Ping
- -Source Routing
- -Internal Source Address
- -Bad Boy List

Level 2 Security - Backbone (Installation Infrastructure)

Installation Level Policy Enforcement and Session State Awareness

- -Deny Un-established Connections
- -Drop packets not associated with session

Level 3 Security - Enclave (Organization/Office)

Organization Level Policy Enforcement

- -Specific to Organization
- -Definable and Enforceable
- -May include service Proxies
- -Email Server Anti-Virus/Malicious Code Detection

Level 4 Security - System /Host (OS & Application)

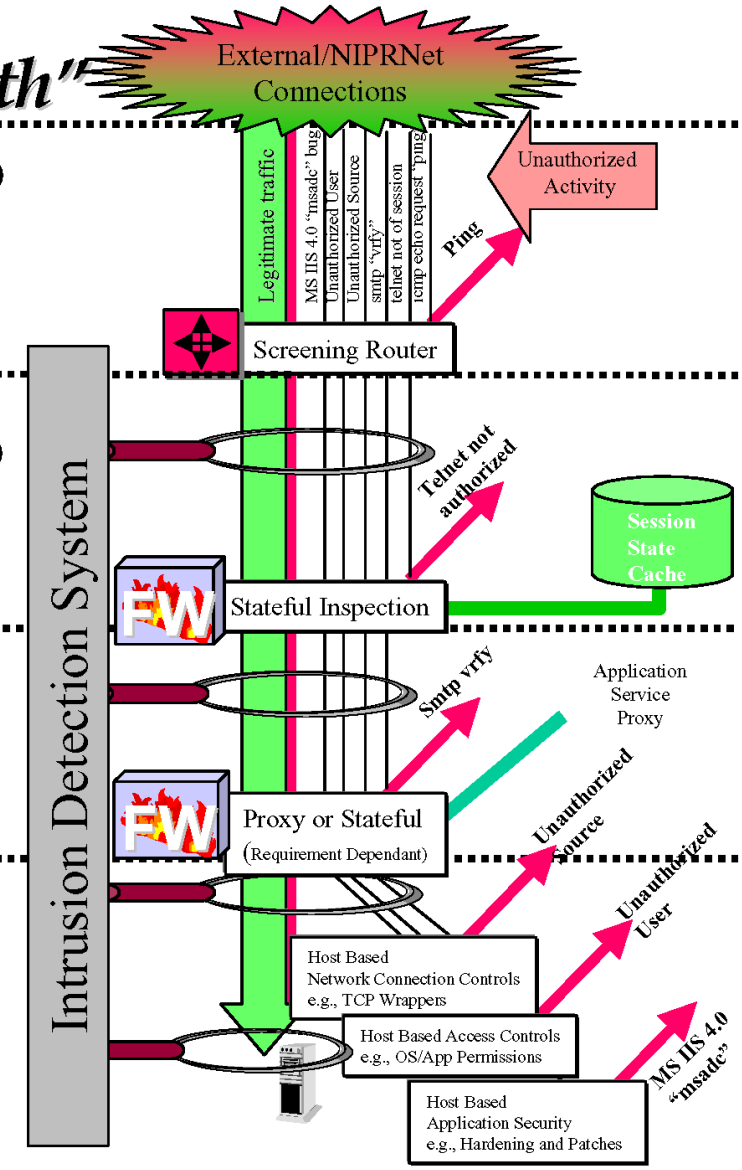
Information System Specific Policy Enforcement

- -Operating Systems Hardening
- -Network Connection Acceptance (TCP Wrapper)
- -User ID and Authentication
- -Application Security

System Vulnerability Assessment and Correction

Password control

Anti-Virus



Accreditation

The official management authorization to operate an IS or network and is based ...on the formal certification of the degree to which a system meets a prescribed set of security requirements. (AR 25-2)

Certification

A comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards made in support of the accreditation process. It establishes the extent to which a particular design and implementation meets a set of specific security requirements.

Designated Approving Authority (DAA)

- Official with the authority to formally assume responsibility for operating an AIS or network at an **acceptable level of risk.**
- Designated before the system design process begins to ensure applicable security requirements are integrated into the proposed AIS.
- Be a US Citizen
- Hold a security clearance with level of information processed by system in jurisdiction

Information System (IS)

Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and that includes computer software, firmware, and hardware.

Security Modes

- A mode of operation in which the DAA accredits an IS to operate (DoD 5200.28) based on the sensitivity of the information and the clearance level of the users
- To determine the security processing mode:
  - **Dedicated.** Users have required clearance, formal access approval, and need to know of information processed
  - **System High.** Users have required clearance, but not necessarily a need to know for all information processed.
  - **Compartmented.** Users have required clearance, but not necessarily formal access approval for all info processed
  - **Multilevel Security.** NOT all users have the the required clearance, formal access approval, or need to know of all information.

Required Security Documents

Describe the operational environment, as well as the automated and procedural safeguards required of the system and users to insure the system is operated at the **accepted level of risk**.

- System Security Authorization Agreement
- Security Policy

Risk

The probability that a particular threat will exploit a particular vulnerability of an information system or telecommunications system.

The Accreditation Process - Backwards Planning

- What information does the DAA need to make a rational decision?
  - The Risk.
    - What is the risk to the individual system, and what risk am I imposing on the DII if I allow this system to operate.
  - The Environment
    - Where is this system operated, who are the operators
  - The Safeguards
    - What measures have been engineered and integrated into this system to mitigate the risk.

Develop a DAA Structured Process

Suggested DAA Contributions

- A well defined Security Policy
  - As a DAA generally covers multiple systems with a similar functional responsibility there should be an area wide security policy
- A well defined Accreditation Master Plan
  - A roadmap for accrediting a system under this DAA
    - What information (documents and format) does the DAA want to insure that he has the necessary information
    - What is the timeline for actions and document submission
- Active Oversight
  - Quarterly DAA level IA IPT

Successful System Approaches

Establish System Accreditation working groups

- Purpose
  - Provide a forum for all interested parties to formulate plans, assign responsibilities, and jointly work issues. This will also be the group that forms the basis of the Risk Management Review Team
- Participants
  - PM, Security Engineer, Certification Authority, Functional Proponent, User Representative, System Developer, DAA

From the Beginning (1 of 2)

- Convene a meeting of the System Accreditation working group (SAWG) as early as possible
  - Initial Focus (likely just PM and Functionals)
    - Determine System Functional Requirements
      - What does the system do
      - The environment the system will be operated in
      - Who does it need to communicate with
      - Determine Users and Sensitivity of Information
    - Determine Mode of Operation
    - Determine DAA

From the Beginning (2 of 2)

- Determine Initial Set of Security Requirements
  - DoD, DA and DAA Security Requirements and Policies
  - Determine if there are any system unique requirements
- Coordinate for Security Engineering Support
- Discuss Certification
  - How will the system be certified
  - Who will certify the system
- Appoint Pre-Deployment ISSM
  - Responsible for securing the system prior to fielding
- Draft System Security Authorization Agreement
  - Defines roles and responsibilities, continually updated

Policy and Requirements Definition

- Develop System Security Policy
  - Defines system unique policy statements
    - Becomes appendix to SSAA
    - Early DAA look into how PM intends to build system
- Develop System Security Requirements
  - Specific list of security requirements that system must meet
    - DoD, DA, and DAA security requirements and policies
    - Basis for assigning responsibility for accomplishing requirements, e.g, procedure, SW, Training
    - Document non applicable requirements

Policy and Requirements Definition

Example C2 Requirements

- C2 is a Security Class from the Orange Book Term that describes the minimum requirements for Controlled Access Protection. Note: The Orange Book is being replaced by Common Criteria
- Discretionary Access Control
  - System shall control access between users and objects
- Accountability
  - Identification and Authentication- All users shall identify themselves before taking any action.
  - Auditing- The system will create, maintain and protect an audit trail sufficient to recreate a user's activity
- Documentation
  - SFUG, TFM, Test Documentation, Design Documentation

Requirements Allocation

Reconvene SAWG (full group)

- Agree on requirements
- Discuss approach to meeting requirements
  - Automated, procedural, development, training
- Lifecycle planning
  - What features are scheduled for what time
  - Feeds resource requirements
- Assign requirements to appropriate parties
- Certification Authority begins planning

Spiral Development (1 of 3)

- Continually Reassess
  - During this design phase the requirements, threats and vulnerabilities will continually be assessed.
- Periodic SAWG Meetings
  - Determine status, reassign requirements, keep DAA informed
  - Function as Risk Management Review Team
    - As issues arise assess impact, develop approaches to mitigate, revise build requirements

Spiral Development (2 of 3)

- Security Engineering
  - not just about producing the necessary documents
  - Security Engineers must:
    - Understand the technical aspects of the system
    - Understand the developmental and operational environments
    - Help define security requirements into System Reqts
    - Research, evaluate, recommend and integrate security solutions into the system development
    - Document the results

Spiral Development (3 of 3)

- Develop and Revise Documents
  - Security Engineer
    - SSAA, Security Policy, Security Features User's Guide (SFUG), Risk Management Review
  - Certification Authority
    - Certification Test Plan, Certification Test Procedures
- Security Testing
  - Use automated tools to assess technical security status, e.g, SPI, ISS. Modify system as necessary within constraints of functional requirements

Certification Testing

- PM believes the system is ready to be formally tested begins the Certification Testing phase
  - Technical
    - Laboratory analysis and testing of system to determine the extent to which the system meets it’s security requirements.
  - Operational
    - Whenever possible, certification testing should also be done in an operational environment.
      - This provides feedback on the training and ability of the operators to execute the SFUG and TFM activities

Post Certification Testing

- Certification Report of Findings (CROF)
  - The Certification Authority presents a detailed report on the ability of the system to meet it’s requirements
- Risk Management Review
  - The SAWG should meet again and review the CROF.
    - Identify remaining vulnerabilities, threats and assign a risk.
    - Develop countermeasures for remaining risks
  - Decision
    - Go forward with accreditation, or redesign & retest.

Submission

- Finalize Documents for submission
- Submit the SSAA, with the security policy, SFUG, TFM, and System Risk Management Review to the DAA
  - Allow 45 days from the date of required Accreditation for DAA review
  - Work with DAA to answer questions, revise documents, or implement new countermeasures

The Decision

At this point the DAA must decide whether or not to accredit the system for use in a specific environment, in a specific mode, with the identified safeguards.

- DAA accepts residual risk, for the individual system and all other systems that interface with that system, and all systems using common services used by this system
- Factors: Likelihood of exploitation, cost to reduce risk, operational necessity of system.

Post Accreditation

- Fielded unit assumes responsibility
- PM likely continues development of next version
- Re-accreditation

Every three years, or within three months of:

- addition or replacement of major component
- change in mode or classification level
- significant change to the operating system
- significant change to threat or available safeguards

Computer Security Standards

- Department of Defense Directive 8500.1 (rescinds the Orange Book)
- Common Criteria/ISO 15408
- ISO 17799

DoDD 8500.1

Establishes policy and assigns responsibilities under reference Section 2224 of title 10, United States Code, "Defense Information Assurance Program" to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.

- Original date 24 Oct 02, certified 21 Nov 03

The Orange Book (now rescinded)

- Published Dec 1985
- Purpose
  - Provided a standard to manufacturers as to what security features to build into their new products
  - Provided DoD a metric with which to evaluate the degree of trust that can be placed in computer systems
  - Provided a basis for specifying security requirements in acquisition specifications
- Part of the DOD Rainbow Series
- Two primary categories of requirements
  - Security features themselves
  - Assurance requirements

Common Criteria (1 of 3)

- New standard
  - For specifying and evaluating the security features of computer products and systems
- International Standard
  - ISO 15408
  - Replaces unique criteria in participating countries
    - US (TCSEC), Canada (CTCPEC), Europe (ITSEC)
  - Allows for participating counties to accept evaluations by others, if they so desire
- Basis for National Information Assurance Partnership
  - NIAP is a joint NIST-NSA effort
  - Evaluation program to establish accredited testing facilities

Common Criteria (2 of 3)

Establishes international standard allowing:

- Wider acceptance of standards
- More facilities to do similar evaluations
  - I.e., more products evaluated and available
- Eases vendor burden of building to divergent international standards and then having to submit to multiple evaluations
- Combines the following…

Common Criteria (3 of 3)

- Concept of Protection Profiles (PP)
  - Standardized set of security requirements for use in procurement and development
  - Similar to a RFP in contracting
- Security Targets
  - Developers statement of what the product actually does. Similar to PP, can be used as basis of evaluation
  - Similar to contractor’s response

Outline of the CC (1 of 4)

Part 1 - Introduction and General Model

- Defines concepts and principles
- Provides construct for expressing security objectives, specifications and requirements
- Use of other requirements statements discouraged as it may limit widespread acceptance of the results

Outline of the CC (2 of 4)

Part 2 - Security Functional Requirements

Catalog of “well defined and understood” security functional requirements to be used as standard, organized into classes, families, and components

- Classes
  - High level grouping of families of requirements sharing common focus, e.g., id and authentication
- Families
  - Lower level groupings of requirement components, sharing specific objective, but differing in emphasis, e.g., User Authentication
- Components
  - Lowest selectable requirements that may be included in Protection Profiles, Security Targets, or Packages, e.g., unforgeable user authentication

Outline of the CC (3 of 4)

Part 3 - Security Assurance Requirements

- Catalog of assurance components that can be used as a way of expressing the assurance requirements of IT products and systems
- Also organized into class, family and components like Part 2
- Defines evaluation criteria for PPs and STs
- Presents the 7 Evaluation Assurance Levels (EALs) which comprise the scale for rating the confidence in security products

Outline of the CC (4 of 4)

Evaluation Assurance Levels (EALs) were developed in an effort to maintain participating country previous criteria, e.g., ITSEC Orange Book for US

EAL#	NAME	TCSEC
1	Functionally Tested	C1
2	Structurally Tested	C2
3	Methodically Tested and Checked	B1
4	Methodically Designed, Tested & Reviewed	B2
5	Semi-formally Designed and Tested	B3
6	Semi-formally Verified Design and Tested	A1
7	Formally Verified Design and Tested	

Protection Profiles (1 of 2)

Implementation independent statement of security needs for a set of IT security products

- Standard Terminology that can be developed by user communities, IT product developers, or others. It contains the following:
  - Intro
    - Identification and overview information
  - Target of Evaluation (TOE)
    - Functional description of the IT product and it's purpose
  - TOE Security Environment
    - Description of the intended environment, to include:
      - Assumptions, Threats, Organizational security policy which will be applied to the product

Protection Profiles (2 of 2)

- Security Objectives
  - High level statement of what the product and it's environment are intended to accomplish in covering threats, policy, and assumptions
- IT Security Requirements
  - Detailed statement of security and assurance requirements
- Application Notes
  - Additional supporting documentation
- Rationale
  - Discussion on how the PP is complete and cohesive and how a product built against it would be effective in meeting objectives

Security Target

Statement of security claims for a particular IT security product or system

- Similar in format to the PP, but includes product specific detailed information:
  - Security Requirements
    - May be directly linked to PP, or
    - Direct reference to CC functional or assurance components, or
    - Explicitly stated requirements
- Basis of agreement among all parities as to what the product offers.
  - Basis of evaluation

Miscellaneous

Package

- A reusable combination of security requirement components, functional or assurance, that meet a particular need
- Simplifies putting PP together if there are well understood packages to handle specific requirements, e.g., Identification and Authentication

The Process

- Develop Protection Profile to meet a need
- Developer builds system to meet PP
  - Developer may build a system in the absence of a PP and submit a standalone Security Target
- Developer prepares a Security Target
  - Addresses how it meets a PP
- Developer submits Product, ST,and accompanying documentation to accredited, independent testing lab
- Lab evaluates the ST to see if it is sufficient baseline for evaluation as well as claims of meeting a particular PP
- Lab performs evaluation
- If passes, lab submits package to evaluation authority to validate findings

Why Care?

- Expect to see Security Products in the future have EAL requirements associated with them
  - Already in Blanket Purchase Agreement requirements
- At some point, PMs will need to include standard security requirements and assurance level terminology in acquisition contracts

ISO 17799 (1 of 3)

- Adopted from BS 7799
- Similar in concept to ISO 9001 compliance
  - ISO 9001 requires corporations to formally document there procedures and practices
  - ISO 17799 requires corporations to formally document there security procedures and practices
- Why Important?
  - Governments requiring it – Taiwan, Singapore and Hong Kong
  - Corporations seek it (Citibank, KPMG, Sony, Unisys)
  - Some insurance companies demand it (AIG for cyber-insurance)

ISO 17799 (2 of 3)

- Organizations must address 10 areas
  - Security policy
  - Security organization
  - Asset classification and control
  - Personnel security
  - Physical and environmental security
  - Communications and operations management
  - Access control
  - Systems development and maintenance
  - Business continuity management
  - Compliance

ISO 17799 (3 of 3)

- Problems
  - Does not specify how to implement security for any of the 10 areas
  - Does not specify metrics or methodologies for measuring compliance in any of the 10 areas

DoD Information Technology Security Certifications and Accreditation Process (DITSCAP)

DITSCAP General (1 of 2)

- **Scope** - Applies to the acquisition, operation, and sustaining of any DoD system that collects, stores, transmits, or processes sensitive or classified information.
- **Objective** - The objective is to establish a DoD standard infrastructure-centric approach that protects and secures the entities comprising the Defense Information Infrastructure (DII)

DITSCAP General (2 of 2)

Defines the activities leading to security C&A. The activities are grouped together in a logical sequence. This Instruction presents the objectives, activities, and management of the DITSCAP process.

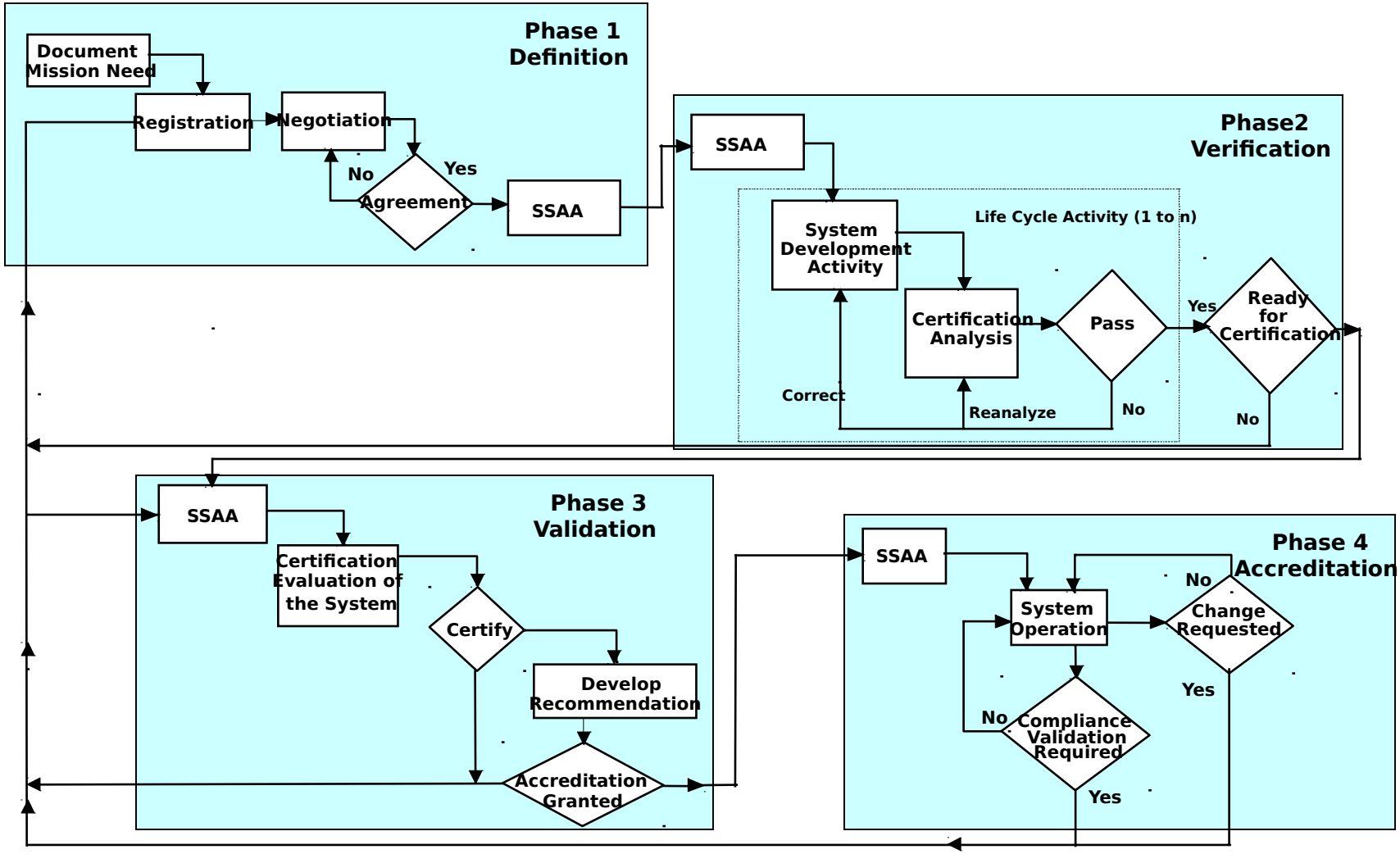
DITSCAP Documents

- **DOD Instruction 5200.40 DITSCAP**
  - Actual Instructions requiring DITSCAP and assigning responsibilities
  - Also provides process overview
  - This brief is prepared from the process overview
- **DOD Manual 5200.40-M**
  - Stand Alone reference manual for implementing DITSCAP
  - Provides more detailed information than the DODI

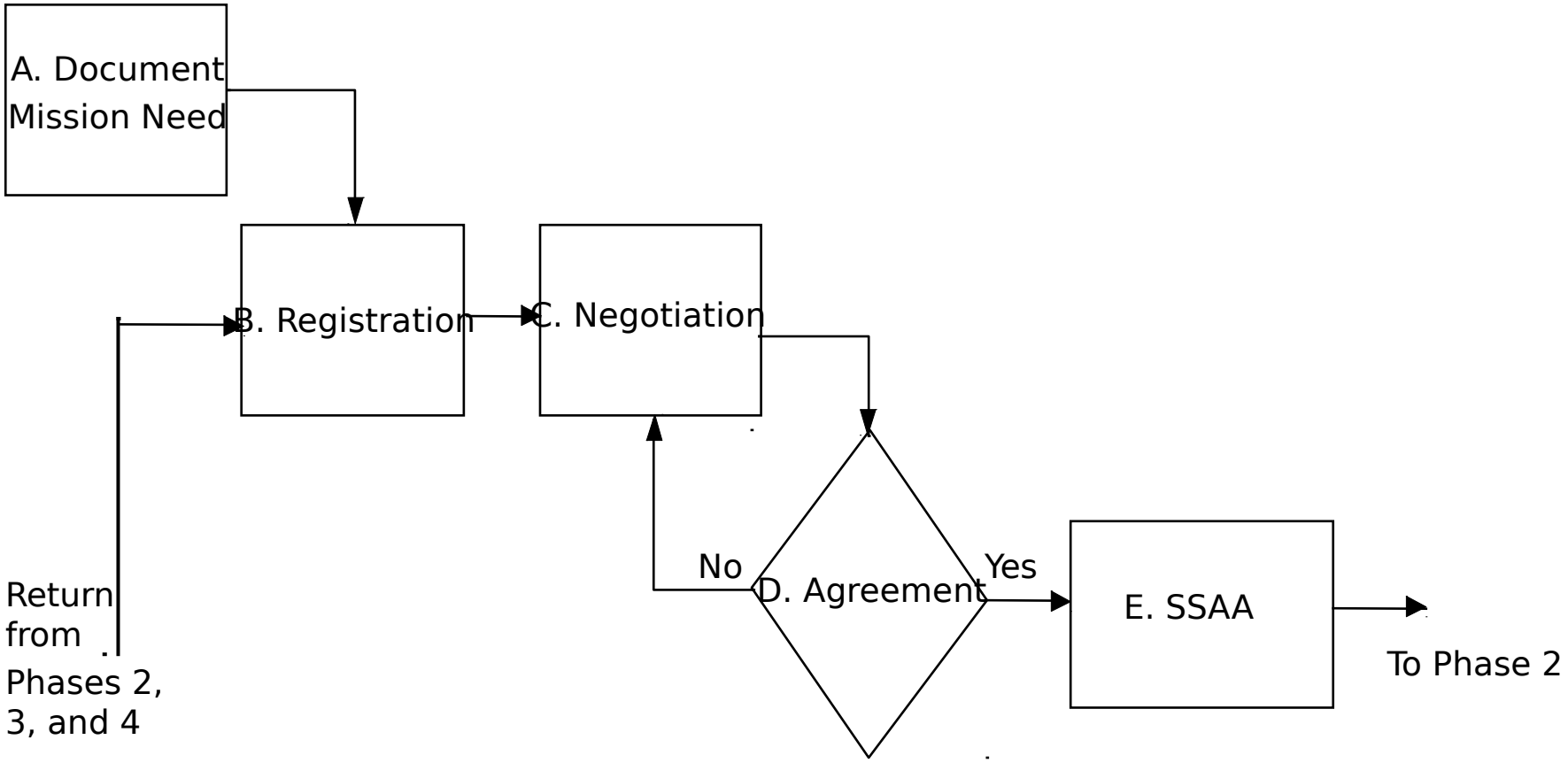
Four DITSCAP Phases

- Phase 1, **Definition**
  - Activities to verify the mission, environment, threat, DAA, CA and security requirements
- Phase 2, **Verification**
  - Activities to verify compliance with security requirements
- Phase 3, **Validation**
  - Determination of residual risk
- Phase 4, **Post Accreditation**
  - Activities to ensure residual risk level is preserved

C&A Phases


Phase 1
Definition
Document
Mission Need
Registration
Negotiation
No
Agreement
Yes
SSAA
Phase2
Verification
SSAA
Life Cycle Activity (1 to n)
System
Development
Activity
Certification
Analysis
Pass
Yes
Ready
for
Certification
Correct
Reanalyze
No
No
Phase 3
Validation
SSAA
Certification
Evaluation of
the System
Certify
Develop
Recommendation
Accreditation
Granted
Phase 4
Accreditation
SSAA
System
Operation
No
Change
Requested
Yes
No
Compliance
Validation
Required
Yes

Phase 1 - Definition Activities



A. Document Mission Need

States system requirements and a description of capabilities including:

- Functions
- Desired interfaces
- The information to be processed.
- The operational organizations supported.
- The intended operational environment.
- The operational threat.

B. Registration (1 of 2)

Activity in Phase 1 that initiates the dialogue among the key players.

Including:

1. Inform interested parties that the AIS requires C&A.
2. Prepare mission description and system identification.
3. Prepare the environment and threat description.

B. Registration (2 of 2)

4. Determine the system security requirements.
5. Identify organizations.
6. Layout the DITSCAP tasks.
7. Develop the draft SSAA.

C. Negotiation

The participants involved in the information systems development, acquisition, operation, security certification, and accreditation agree on the implementation strategy to be used to satisfy the security requirements identified during system registration.

- Review initial SSAA.
- Conduct the certification requirements review.
- Approve final SSAA.

D. Agreement

Between the DAA, CA, PM, SE, and the user representative. It should:

- specify ITSEC requirements
- document certification tailoring
- level of effort
- identify possible solutions
- maintain operational systems security

E. SSAA Contents

- The formal agreement.
- All requirements necessary for accreditation.
- All security criteria for use throughout the IT system life-cycle.
- The DITSCAP plan.

SSAA Format (1 of 5)

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION
    - 1.1. System name and identification
    - 1.2. System description
    - 1.3. Functional description
        - 1.3.1. System capabilities
        - 1.3.2. System criticality
        - 1.3.3. Classification and sensitivity of data processed
        - 1.3.4. System user description and clearance levels
        - 1.3.5. Life-Cycle of the system
    - 1.4. System CONOPS summary

2. ENVIRONMENT DESCRIPTION
    - 2.1. Operating environment
    - 2.2. Software development and maintenance environment
    - 2.3. Threat description

SSAA Format (2 of 5)

3. SYSTEM ARCHITECTURAL DESCRIPTION
    - 3.1. Hardware
    - 3.2. Software
    - 3.3. Firmware
    - 3.4. System interfaces and external connections
    - 3.5. Data flow (including data flow diagrams)
    - 3.6. TAFIM DGSA security view
    - 3.7. Accreditation boundary

4. ITSEC SYSTEM CLASS
    - 4.1. Interfacing mode
    - 4.2. Processing mode
    - 4.3. Attribution mode
    - 4.4. Mission-reliance factor
    - 4.5. Accessibility factor
    - 4.6. Accuracy factor
    - 4.7. Information categories

SSAA Format (3 of 5)

5. SYSTEM SECURITY REQUIREMENTS
    - 5.1. National/DoD security requirements
    - 5.2. Governing security requisites
    - 5.3. Data security requirements
    - 5.4. Security CONOPS
    - 5.5. Network connection rules
        - 5.5.1. To connect to this system
        - 5.5.2. To connect to the other systems in the CONOPS
    - 5.6. Configuration and change management requirements
    - 5.7. Re-accreditation requirements

6. ORGANIZATIONS AND RESOURCES
    - 6.1. Identification of organizations
        - 6.1.1. DAA
        - 6.1.2. Certification authority
        - 6.1.3. User representative
        - 6.1.4. Organization responsible for the system

SSAA Format (4 of 5)

6.2. Resources
6.2.1. Staffing requirements
6.2.2. Funding requirements
6.3. Training for certification team
6.4. Roles and responsibilities
6.5. Other supporting organizations or working groups

7. DITSCAP PLAN

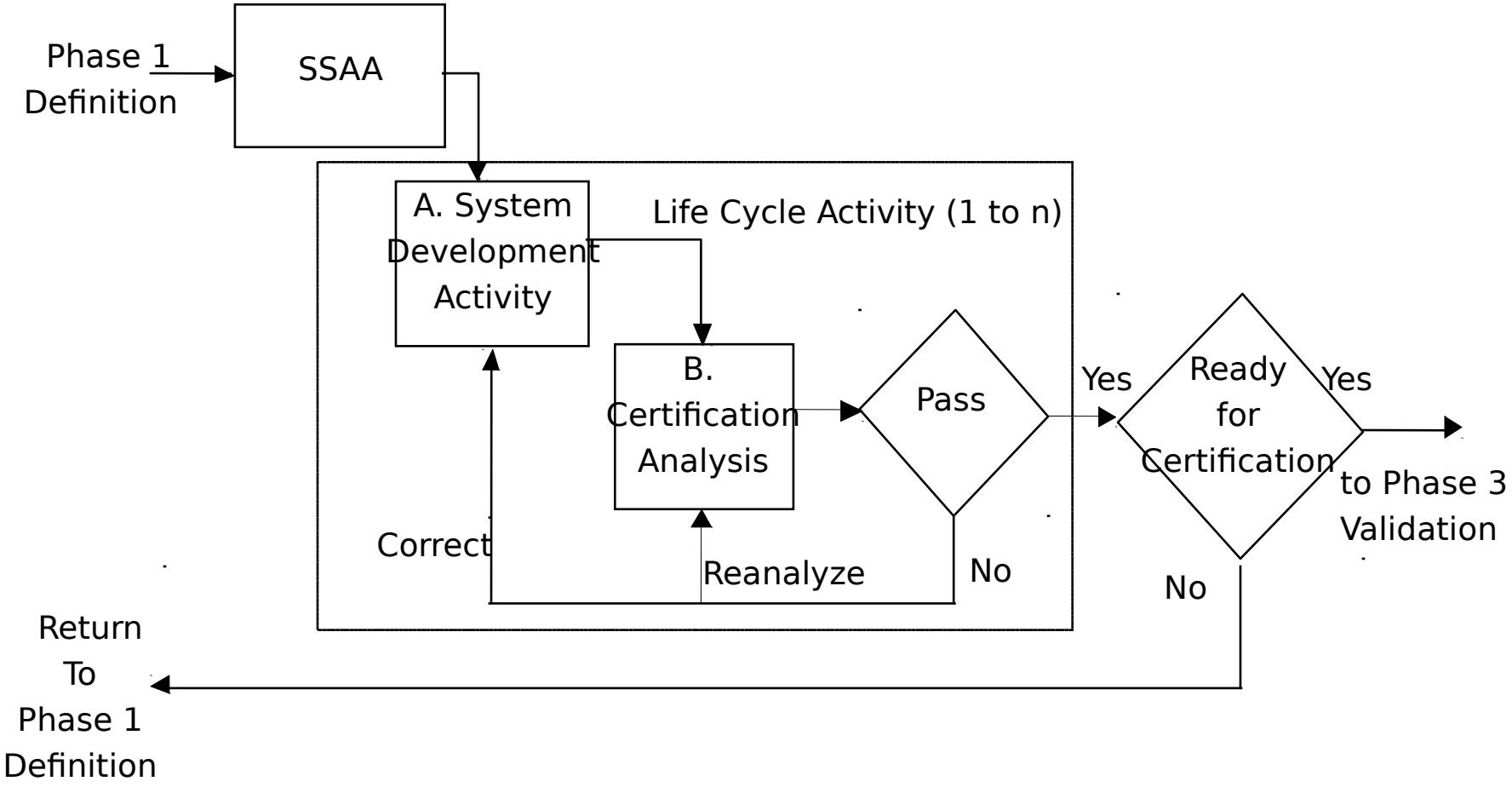
7.1. Tailoring factors
7.1.1. Programmatic considerations
7.1.2. Security environment
7.1.3. IT system characteristics
7.1.4. Reuse of previously approved solutions
7.1.5. Tailoring summary
7.2. Tasks and milestones
7.3. Schedule summary
7.4. Level of effort
7.5. Roles and responsibilities

SSAA Format (5 of 5)

AP1.1.2. Appendices. Appendices should include system C&A artifacts. Optional appendices may be added to meet specific needs. Include all documentation relevant to the systems' C&A.

A Acronym List
B Definitions
C References
D Security Requirements and/or Requirements Traceability Matrix
E Security Test and Evaluation Plan and Procedures
F Certification Results
G Risk Assessment Results
H CA's Recommendation
I System Rules of Behavior
J Contingency Plan(s)
K Security Awareness and Training Plan
L Personnel Controls and Technical Security Controls
M Incident Response Plan
N Memorandums of Agreement - System Interconnect Agreements
O Applicable System Development Artifacts or System Documentation
P Accreditation Documentation and Accreditation Statement

Phase 2 - Verification Activities



Phase 2 Verification

Process activities of phase 2; verify the evolving system's compliance with the requirements agreed on in the SSAA.

- Continuing refinement of the SSAA.
- System development or modification.
- Certification analysis

A. System Development

- The activities required to develop and integrate the IT system components.
- Each activity task has a corresponding phase 2 certification analysis task.

B. Certification Analysis (1 of 3)

Determines if the IT system is ready to be evaluated and tested under phase 3, validation:

1. System architecture
2. Software design
3. Network connection rule compliance
4. Integrity of integrated products
5. Life-cycle management
6. Vulnerability assessment

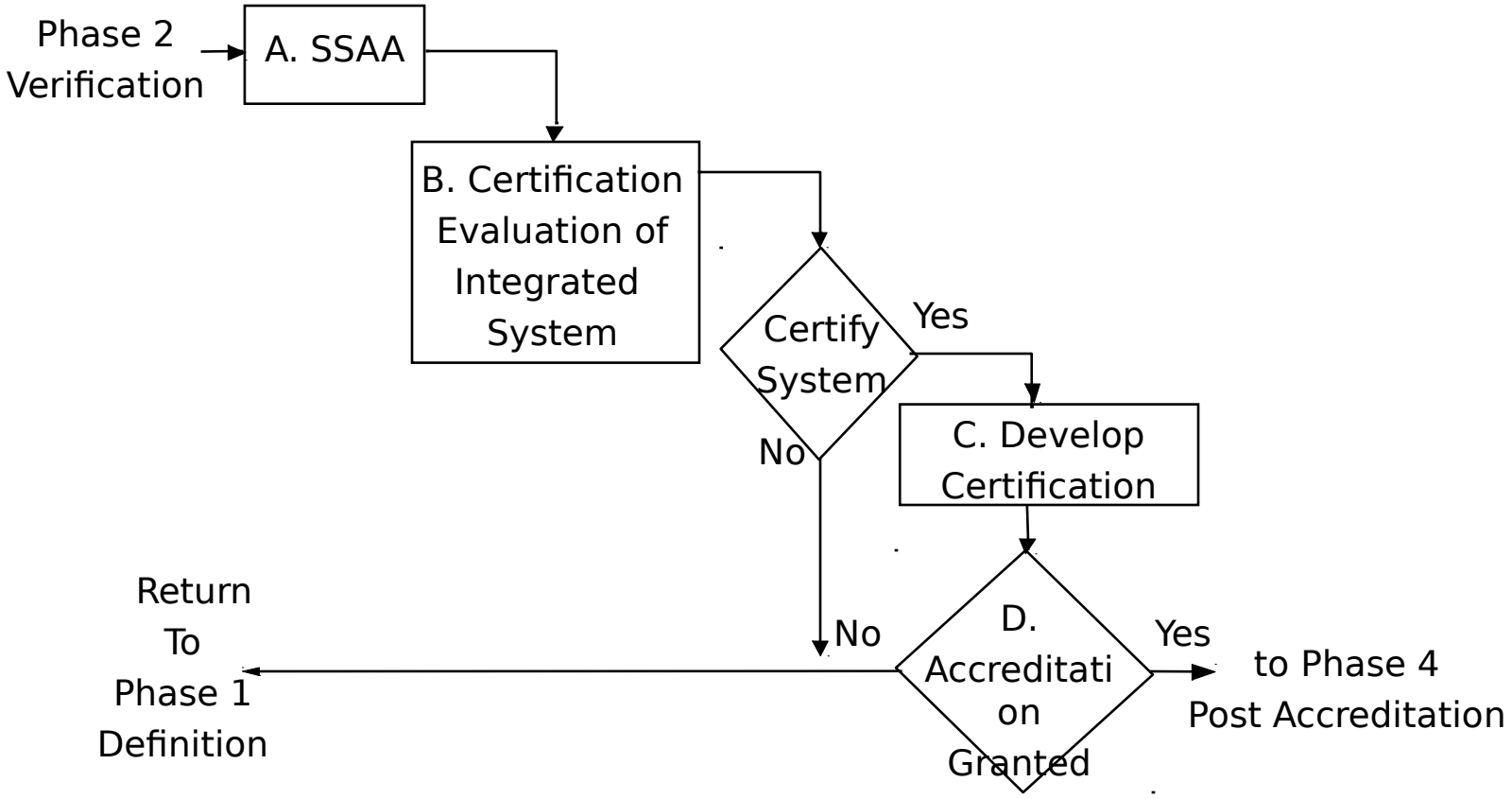
B. Certification Analysis (2 of 3)

1. **System architecture** - ensures compliance with the architecture description in the SSAA.
2. **Software design** - evaluates how well the software reflects the security requirements of the SSAA and the security architecture of the system.
3. **Network connection rule compliance** -evaluates connections of an AIS to a network to determine that the system will not adversely affect the security of the network.

B. Certification Analysis (3 of 3)

4. **Integrity of integrated products** - evaluates integration of COTS, GOTS, or NDI software to ensure that their use complies with the system security architecture, while maintaining the integrity of each product.
5. **Life-cycle management** - ensures change control and configuration management practices are in place and sufficient to preserve the integrity of the security software and hardware.
6. **Vulnerability assessment** - with regard to confidentiality, integrity, availability, and accountability and recommends countermeasures.

Phase 3 - Validation Activities



Phase 3 Validation

The process activities of phase 3 validate that the preceding work has produced an information system that operates in a specified computing environment with an acceptable level of residual risk:

- Refining the SSAA.
- Evaluating the integrated IT system.
- Certification
- Accreditation

A. Refining the SSAA

Phase 3 begins with a review of the SSAA to ensure that its requirements and agreements still apply.

At each stage of the integrated IT system’s acceptance, the SSAA is refined by adding details to reflect the current state of the system.

B. Certification Evaluation of the System

This process certifies that the fully integrated and operational system complies with the requirements stated in the SSAA and may be operated with an acceptable level of residual risk.

C. Certification Evaluation

Certification tasks include certification of the software, firmware, and hardware and inspections of operational sites to ensure compliance with the physical security, procedural security, TEMPEST, and COMSEC requirements.

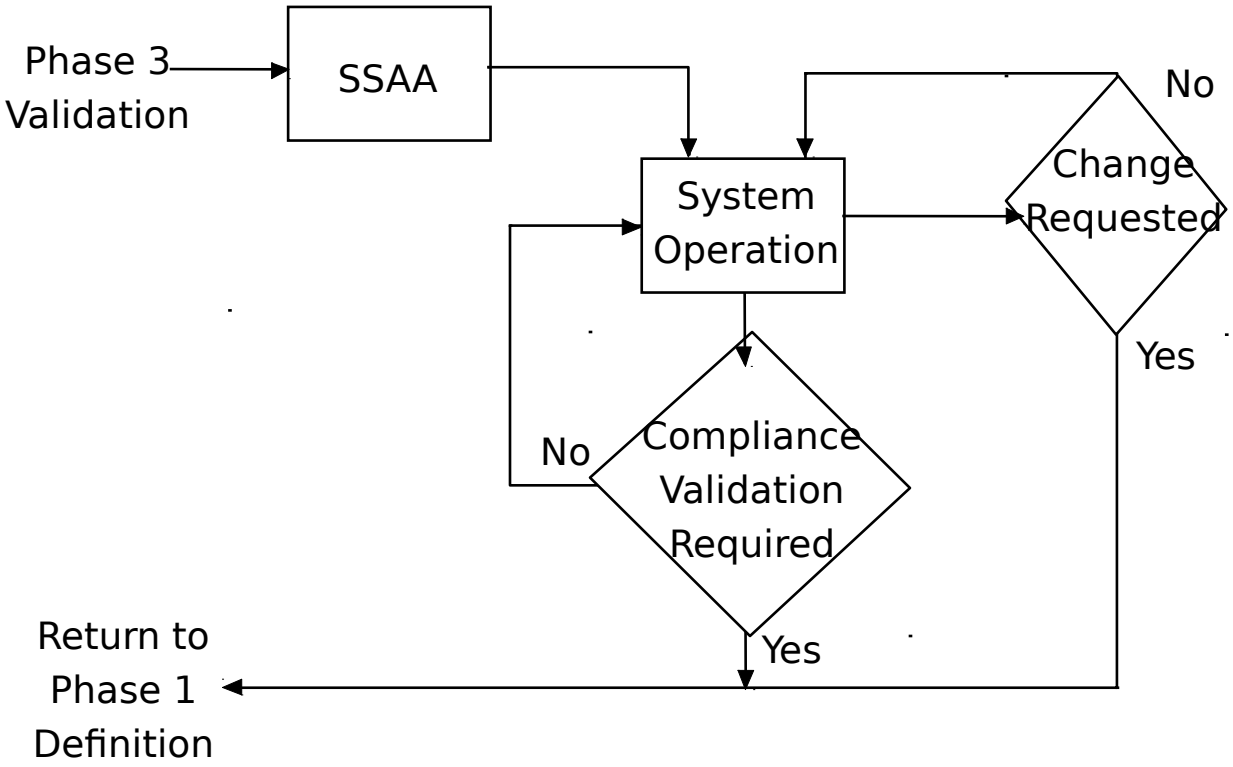
Certification Evaluation Tasks

1. Security Test and Evaluation.
2. Penetration testing.
3. TEMPEST and Red-Black verification.
4. Validation of COMSEC compliance.
5. System management analysis.
6. Site accreditation survey.
7. Contingency plan evaluation.
8. Risk-based management review

D. Accreditation

- At the completion of all certification tasks a decision by the DAA is required.
- This includes:
  - CA's recommendation
  - DAA authorization to operate
  - supporting documentation
  - SSAA
- When a decision is made to accredit the system, phase 4 Post Accreditation begins.

Phase 4 - Post Accreditation



Phase 4 Post Accreditation

Process activities necessary to continue to operate and manage the system so that it will maintain an acceptable level of residual risk. These activities are:

1. Ongoing maintenance of the SSAA.
2. System operation.
3. Change management.
4. Compliance validation.

DITSCAP Management Approach

- Focuses on management at the applicable systems level to execute DITSCAP for a given system.
- Concept includes system program or operations management, senior operational staff, users, and working level security managers.

DITSCAP Roles

(Signatories to the DITSCAP)

1. System Program Manager.
2. Designated Approving Authority.
3. Certification Agent.
4. User Representative.

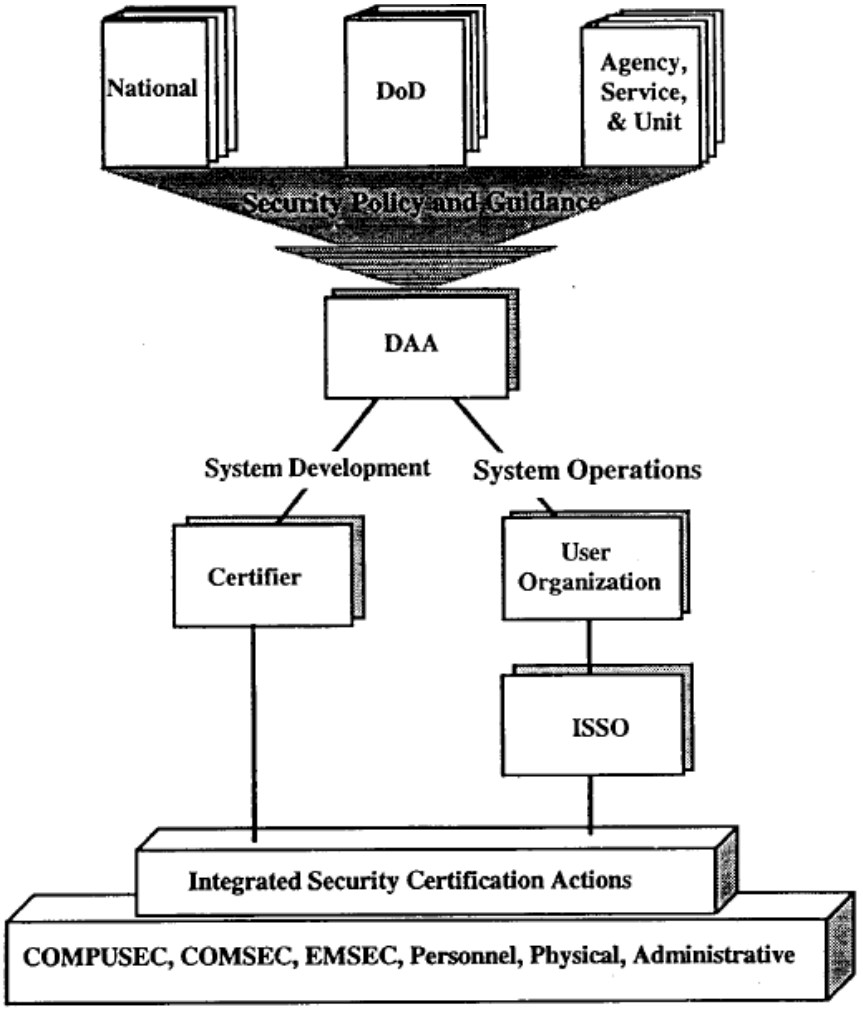
DITSCAP Overview

- Identifying the roles, components, phases, activities, tasks, and steps and explaining their interrelationship to achieve accreditation.
- The DITSCAP establishes a DoD standard infrastructure-centric approach that protects and secures the DII.
- Standardizing the process minimizes risks associated with nonstandard security implementations across shared infrastructure and end systems.

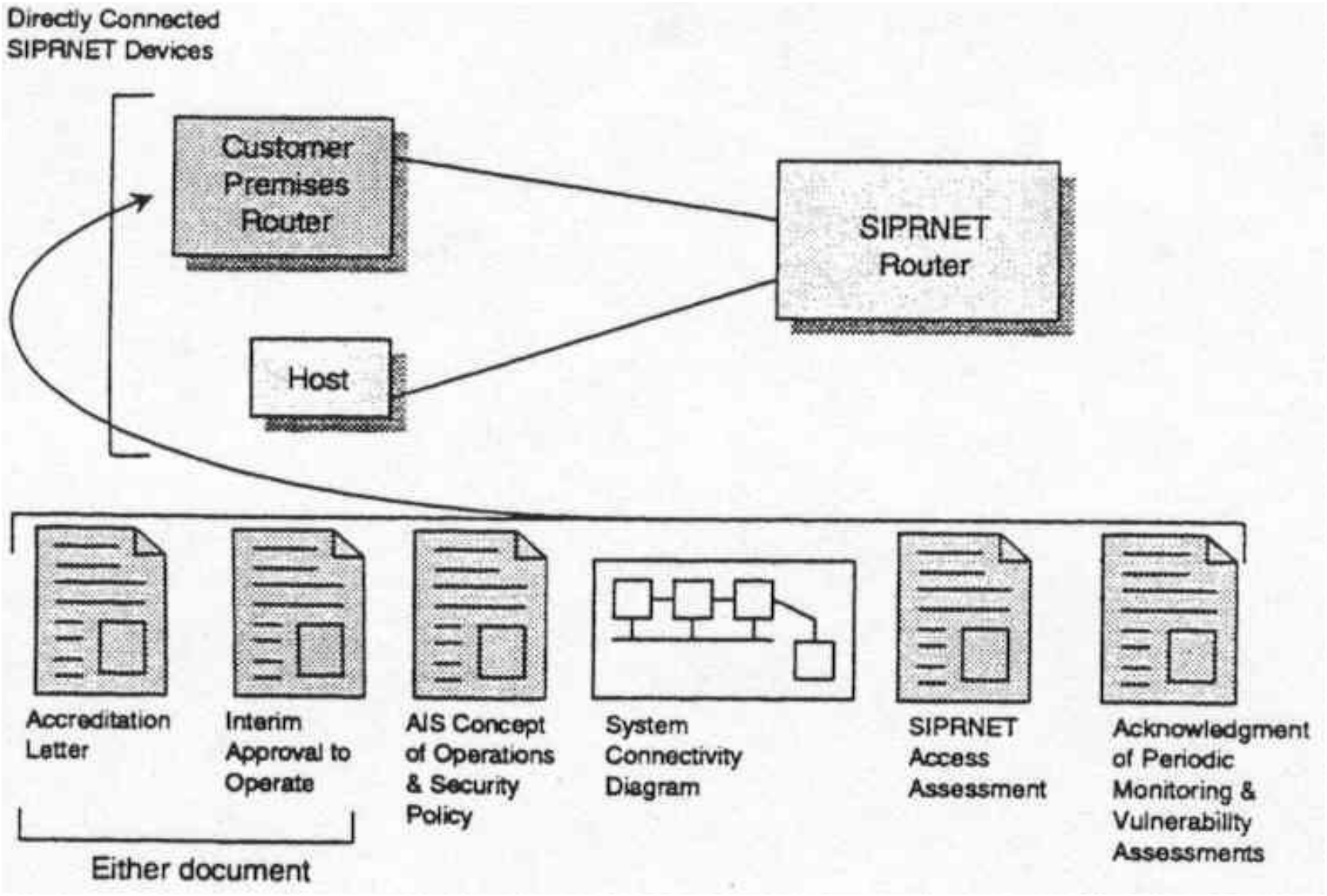
National Information Assurance Certification and Accreditation Process (NIACAP)

- Established the minimum national standards for certifying and accrediting national security systems
- Same process as DITSCAP
- Three types of NIACAP accreditation
  - Site accreditation
  - Type accreditation
  - System accreditation

Security Management Relationships



SIPRNET Accreditation Process



SIPRNET Requirements (1 of 2)

- Letter of accreditation or Interim Authority to Operate (IATO)
- Site system connectivity diagram
- Consent to Monitor Statement
- Statement of significant or residual risk
- Non-DoD, foreign, or contractor connections require Joint Staff approval
- Statement of minimum security requirements

SIPRNET Requirements (2 of 2)

- Statement of specific security features and implementations
- Copies of any Memorandums of Understanding/ Agreement (MOA/MOU) with interconnected systems/networks
- Mode of Operations
- Maximum level of sensitivity of information processed
- Completed Foreign Access Questionnaire
- IP Registration

Letter of Accreditation Requirements

The accreditation grants approval for the operation of the system. The letter contains:

- the organization's letterhead and date of signature
- security mode of operations and specified data sensitivity or classification level
- a prescribed set of safeguards
- a defined threat and stated vulnerabilities
- stated interconnections to other systems
- a defined level of risk
- a specified period of time
- a specified suite of hardware and software
- a specified operating environment
- signature and signature block of DAA

Letter of Accreditation

CINCs/Services/Agency's Name

[Address]

Date

SUBJECT: Accreditation of CINCs/Services/Agency's Name Workstation/network

Ref: (a) Accreditation Support Documentation

1. In accordance with the provisions of [CINCs/Services/Agency's Name] Instruction [XXX-XXX-XX], authorization is hereby granted for the operation of the [CINCs/Service/Agency's Name Network/Workstation], located in [Building 0000, Suite 000, Address]. This accreditation is based upon a review of the information provided in reference (a). This accreditation is valid as long as the Baseline Security Safeguards defined in the [CINCs/Services/Agency's specific security directives and guidelines] are implemented. This system is authorized to operate in the threat environment defined in reference (a) and with stated vulnerabilities as identified in the [CINCs/Services/Agencies] Baseline Security Documents. The accredited system consists of [list equipment here] This system is authorized to process [Place Maximum mode of operation level processed]. The CINCs/Services/Agencies' network/workstation is connected to the SIPRNet and [Place any other network that the system is connected to].

2. This accreditation is valid for 3 years from the date of this letter. Reaccreditation is required sooner if there is any change that affects the security posture of the system. It is the responsibility of the senior official in charge of the system to ensure that any change in threat, vulnerability, configuration, hardware, software, connectivity, or other modification is analyzed to determine its impact on system security. Appropriate safeguards will be implemented to maintain a level of security consistent with the requirements of this accreditation.

3. The undersigned accepts the risk for the operation of the CINCs/Services/Agencies' system defined above.

Signature

Designated Approving Authority
CINCs/services/Agencies' Name

Letter of IATO Requirements

Gives temporary authorization to process information under defined conditions; containing:

- Organization’s letterhead and date of signature
- specified security mode of operations; data sensitivity or classification level
- defined security safeguards
- a defined threat and stated vulnerabilities
- Stated interconnection to other systems
- Statement of acceptance of risk for the system
- period of duration
- hardware and software platform
- operational environment
- Signature and signature block of DAA

IATO

CINCs/Services/Agency's

Address

Date

SUBJECT: Interim Approval to Operate [CINCs/Services/Agency's] network/workstation

Ref: (a) Accreditation Support Documentation

1. In accordance with the provisions of [CINCs/Services/Agency's] Instruction xxx-xxx-xx, an Interim Approval to Operate (IATO) is hereby granted to the [CINCs/Services/Agency's] Network, located in Building 000, Suite 000, [Address]. This IATO is based upon a review of the information provided in reference (a). This IATO is valid as long as the Baseline Security safeguards defined in the [CINCs/Services/Agency's specific security directives and guidelines] are implemented. This system is authorized to operate in the threat environment defined in reference (a) and with stated vulnerabilities as identified in the [CINCs/Services/Agency's Baseline Security Documents]. The IATO system consists of the [equipment list]. This system is authorized to process [Place Maximum mode of operation level processed] . The [CINCs/Services/Agency's] network is connected to SIPRNet and [place any other network that may be connected to].

2. This IATO is valid for 90 days from the date of this letter. Final accreditation action is required before the expiration of this IATO. This IATO will terminate sooner if there is any change that affects the security posture of the system. It is the responsibility of the senior official in charge of the system to ensure that any change in threat, vulnerability, configuration, hardware, software, connectivity, or other modification is analyzed to determine its impact on system security. Appropriate safeguards will be implemented to maintain a level of security consistent with the requirements of this IATO.

3. The undersigned accepts the risk for the operation of the [CINCs/Services/Agency's] system defined above.

Signature

Designated Approving Authority
CINCs/Services/Agency's

Connectivity Description Diagram Requirements

All associated hardware devices: hubs, bridges, routers, switches, guards, firewalls, gateways, modems, encryption devices, card readers, backup devices, surge protectors and UPS.

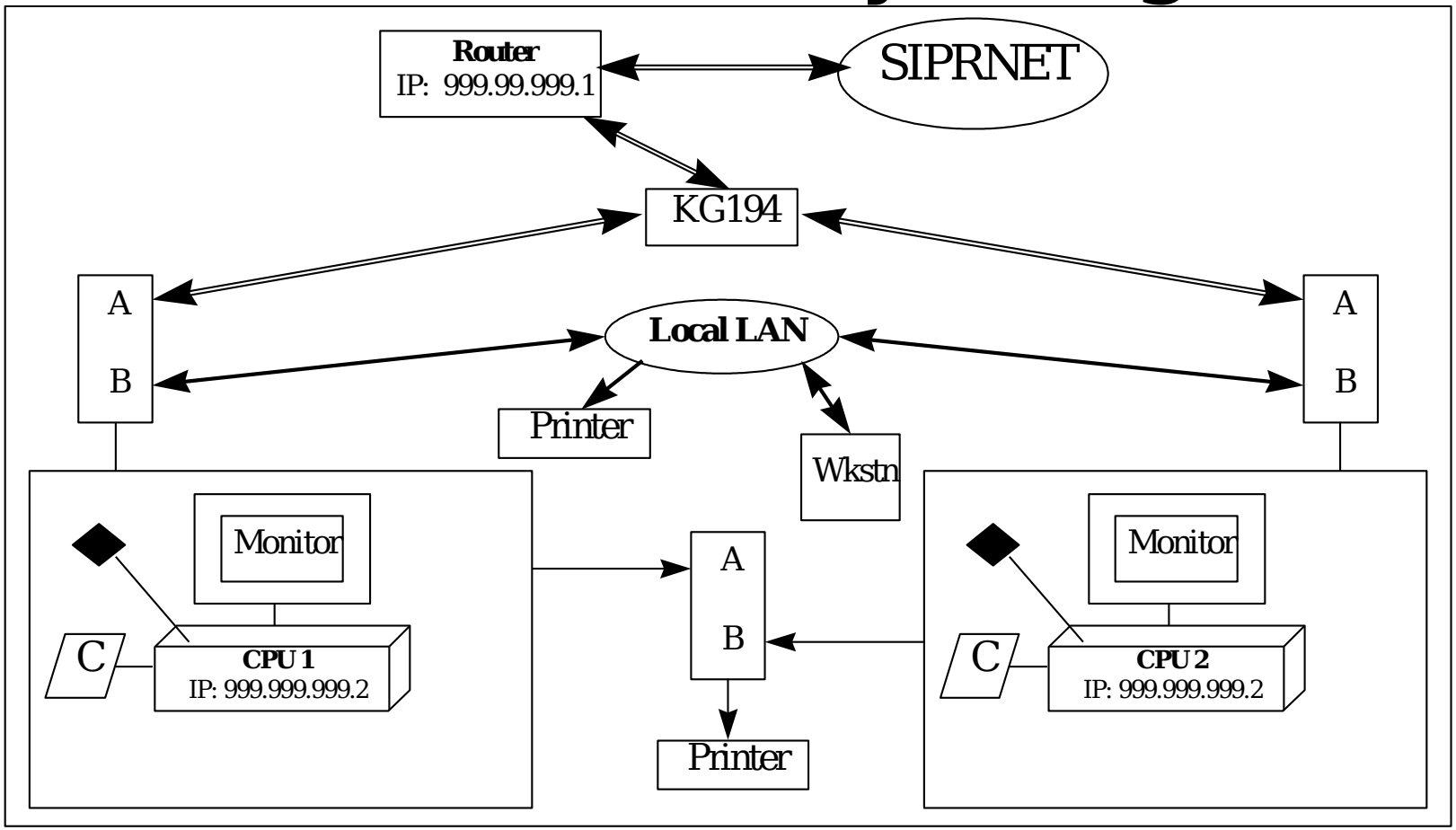
Actual and planned interfaces to internal and external LANs and WANs

SIPRNet connections

Flow of information to, from and through all connections

Router Port number (RTRP), host IP address and CCSD number if known.

Sample Connectivity Diagram



Legend

Surge Protector

Secret LAN

SIPRNET

Card Reader

C

Consent to Monitor Statement Requirements

- Date of statement
- Consent to monitor heading
- CJCS Instruction reference
- Statement acknowledging DISA will conduct periodic monitoring of SIPRNet and consent to conducting initial and unannounced vulnerability assessments
- CINCs/Services/Agency’s site name
- Senior official’s signature

Sample
Consent to Monitor Statement

Date

CONSENT TO MONITOR

In Accordance with the requirements of Chairman Joint Chief of Staff Instructions (CJCSI) 6211.02, Defense Information System Network and Connected Systems, 23 June 93, and DISN Secret Internet Protocol Router Network (SIPRNET) connection requirements, we acknowledge that the Defense Information Systems Agency (DISA) will conduct periodic monitoring of SIPRNET. We acknowledge and consent to DISA conducting an initial vulnerability assessment and periodic unannounced vulnerability assessments on our connected host systems to determine the security features in place to protect against unauthorized access or attack.

Signature

Chief Network Official
[CINCs/Services/Agency's Name]

Statement of Residual Risk Requirements

Letterhead

Date

Statement of risk

Assessment of risk to IA principals

Assessment of system vulnerabilities

Evaluation of operational procedures and safeguards

Statement of Residual Risk

CINCs/Services/Agency's
Address

Date

SUBJECT: Statement of Residual Risk

1. The residual risk to the CINCs/Services/Agency's is [minimal or other]. This assessment is based on an evaluation of the known and presumed threats to the system, the vulnerabilities associated with the CINCs/Services/Agency's system, and all employed protective countermeasures.

2. The risk to system and data confidentiality, integrity, availability, and accountability is being maintained at an acceptable level. The vulnerabilities of the system with respect to the documented threat, ease of exploitation, potential rewards to the threat agent, and probability have been minimized by means of an aggressive Risk Management Program.

3. This Risk Management Program is based on a continual evaluation of the operational procedures and safeguards of the CINCs/Services/Agency's network to determine their effectiveness and ability to offset the defined risk at the CINCs/Services/Agency's site.

Signature

Chief, XX Branch
CINCs/Services/Agency

Red/Black Installation Guide (1 of 2)

- **Primary guidance from NSTISSAM TEMPEST/2-95 dated 12 December 1995**
  - **A separation of one meter should be maintained between any RED processor and:**
    - BLACK equipment
    - BLACK wire lines that exit the inspectable space or are connected to an RF transmitter
    - BLACK power lines
    - Conductors that exit the inspectable space
  - **Separation of 5 centimeters should be maintained between any RED wire line and:**
    - BLACK wire lines that exit the inspectable space or are connected to an RF transmitter (for parallel runs over 30 m increase distance to 15 cm)
    - BLACK power lines
  - **RED and BLACK wire lines should not use a common distribution vehicle**

Red/Black Installation Guide (2 of 2)

- **Red processors should not be powered from the same circuits as BLACK equipment, except when the power lines that exit the inspectable space are equipped with powerline filters**
- **Patch Panels**
  - Jack fields should have incompatible connectors to prevent inadvertent RED to BLACK patching
  - Separate the RED and BLACK by one meter
- **One meter separation is required between different red classifications (i.e. SIPRNET and JWICS, SIPRNET and SECRET – Coalition)**
- **SCIFs usually required a red and black ground**

Red/Black Installation References

- MIL-HDBK-232
- NSTISSAM TEMPEST/2-95

Summary

- Overview
- Defense in Depth
- Terms
- Accreditation Process
- Orange Book – DOD 5200.28 – Trusted Computer Security Evaluation Criteria
- Common Criteria
- DOD Information Technology Security Certification and Accreditation Process (DITSCAP)
- SIPRNET Connection Approval Process
- Red/Black Installation Guide